Received 27 October 2022; revised 12 December 2022; accepted 25 December 2022. Date of publication 28 December 2022;
date of current version 11 January 2023.

Digital Object Identifier 10.1109/OJCOMS.2022.3232753

Analyzing Physical-Layer Security of PLC Systems Using DCSK: A Copula-Based Approach

VINAY MOHAN[1], AASHISH MATHUR[1] (Member, IEEE), AND GEORGES KADDOUM[2] (Member, IEEE)

[1]Department of Electrical Engineering, Indian Institute of Technology Jodhpur, Jodhpur 342037, India

[2]Department of Electrical Engineering, École de technologie supérieure, Montreal, QC H3C 0J9, Canada

CORRESPONDING AUTHOR: A. MATHUR (e-mail: aashishmathur@iitj.ac.in)

ABSTRACT This study analyzes the physical layer security (PLS) performance of a differential chaos shift keying (DCSK) modulation-based Power Line Communication (PLC) system by exploiting the novel Farlie-Gumbel-Morgenstern (FGM) Copula approach. A power line Wyner's wiretap channel model is investigated, where the main channel and the wiretap channel are assumed to be correlated and Log-normally distributed. The Gamma approximation to the Log-normal distribution is employed to simplify the computation. Concurrently, the PLC channel noise is modeled as a Bernoulli-Gaussian random process. Utilizing a Copula based approach to model the dependence among the correlated PLC channels, the PLS performance of the PLC system is evaluated in terms of the secure outage probability (SOP) and the strictly positive secrecy capacity (SPSC). It is revealed through the asymptotic SOP analysis that the secrecy diversity order depends on the shaping parameter (m_{γ_M}) of the main channel. We also propose an algorithm to maximize the secrecy throughput under SOP constraints. Based on the insights from this analysis, it has been seen that the SOP performance degrades when the value of the dependence parameter (θ) increases. Also, the secrecy throughput performance improves with a lower optimal threshold value of the signal-to-noise ratio (SNR), γ_{th}. Furthermore, some other insightful observations are presented by studying the impact of different parameters such as spreading factor (β), impulsive noise occurrence probability (p), transmitted power (P_T), and impulsive noise index (K).

INDEX TERMS Power line communication, physical layer security, secure outage probability, strictly positive secrecy capacity, log-normal distribution, Bernoulli-Gaussian random process, secrecy throughput.

I. INTRODUCTION

OVER the past years, the fourth industrial revolution, also named Industry 4.0, has amalgamated modern information and communication technologies (ICTs) to design a complete, efficient, reliable, robust, optimized, and smart industrial system. Industry 4.0 mainly consists of cyber-physical systems and the Internet of Things (IoT) [1], where multiple devices, machines, vehicles, and buildings connect to each other via the integration of various ICTs. In Industry 4.0, ICTs are required to offer a very good quality-of-service (QoS) for the last mile access ("to the home") and the last inch access ("in the home") [2]. QoS covers various key performance indicators (KPIs) such as better network connectivity, high data rates, low latency, high network coverage, low maintenance and installation cost, cybersecurity, etc. In this context, Power Line Communication (PLC) is a suitable contender for fulfilling the above mentioned KPIs in Industry 4.0. PLC is a wireline technology that allows an exchange of digital data over the existing electric wires or power distribution networks. The notable advantage of PLC lies in its use of the existing ubiquitous wired infrastructure of the power grid, making it a low-cost technology and offering high network coverage. High data rates can be supported by PLC as demonstrated in HomePlug Powerline Alliance (HomePlug) and IEEE P1901 standards for home networking [3]. Moreover, PLC can play a considerable role in IoT applications including smart buildings, smart vehicles, smart grids, and smart industries [3]. Consequently, due to its appealing characteristics PLC technologies play a significant role in Industry 4.0 and IoT networks.

The security of data has always been a salient aspect of telecommunication systems. Serving an impenetrable security is considered an essential part of the QoS index. Specifically, in Industry 4.0 and IoT networks, various devices and machines interconnect through a broadcast communication network. Therefore, accessing a broadcast communication network becomes easy for an intruder. Primarily, data security have been provided by cryptographic techniques and key management mechanisms. In IoT devices, various authentication schemes are being introduced. Recently, software-defined networking authentication schemes have been proposed to protect data in IoT devices [4]. However, due to advancements in computer technology, these cryptographic techniques and key management mechanisms cannot provide unbreakable network security [5].

Recently, the physical layer security (PLS) (also known as information-theoretic security), where the randomness of the communication channels is exploited in the physical layer to prevent data leakage, is a complimentary method that can strengthen digital data security [6]. Initially, the concept of the information-theoretic approach was proposed by Shannon in terms of perfect secrecy [7], then it was carried on by Wyner [8], and after that by Csiszár and Korner [9], who confirmed the information security by using channel codes in a wiretap scenario. A comprehensive study of PLS in random wireless cellular networks has been illustrated in [10], where the key security issues of full-duplex transceivers and multi-tier heterogeneous networks are studied. In [11], the authors modeled multi-antenna transmission techniques for achieving better secure connectivity in random wireless networks over Rayleigh fading channels. Secure communication in stochastic wireless networks was investigated in [12], where the intrinsically secure communication graph method is studied for a large-scale network to establish secure communication in the presence of eavesdroppers. In [13], the PLS performance of stochastic wireless networks was investigated, where maximum secrecy capacity in an intrinsically secure communication graph is characterized by collusion of eavesdroppers. The authors of [14] analyzed the PLS performance of multi-antenna small-cell networks, where the artificial noise method was adopted to enhance the secrecy performance of the cellular network. Recently, in [15], the PLS performance of free space optical communications was investigated over Malaga channels, where different eavesdropping scenarios are presented.

Similar to wireless communication channels, PLC channels are natively broadcast and multipath in nature due to the presence of several branches and impedance mismatches, which cause numerous reflections of the transmitted signal [16], [17], [18], [19], [20]. As a result, the channels are shared by all network users and information tapping becomes more prone to eavesdroppers. Therefore, in this case, secrecy becomes an essential issue in maintaining information confidentiality between the legitimate transmitters and receivers. Hence, providing an adequate security is always an important concern in PLC systems. In [18] and [19], the authors have analyzed and compared the PLS performance of a single-input single-output (SISO) PLC system and a wireless system. It was found that the secrecy rate is lower in PLC systems than in wireless communication systems. In [20], the PLS of a multi-input multi-output (MIMO) PLC system has been evaluated. Here, it was established that MIMO PLC is more secure than SISO PLC systems. The secrecy performance of a cooperative PLC system was investigated over correlated Log-normal communication channels in the presence of a passive eavesdropper in [21]. Similarly, the authors of [22] analyzed the PLS performance of PLC systems in terms of average secrecy capacity (ASC), secure outage probability (SOP), and strictly positive secrecy capacity (SPSC) for independent and correlated channels.

In order to improve the security of communication systems, researchers have also explored different secure modulation schemes. Chaos-based modulation techniques have been widely studied for their impactful advantages over other traditional modulation schemes [23], [24], [25]. Chaotic signals are easier to generate, non-periodic, wide-band, and possess good auto/cross-correlation properties. Furthermore, chaotic modulation schemes provide robustness to multipath fading environments [26], jamming resistance along with a low probability of interception (LPI) [27], and secure communications [28]. Among chaos-based schemes, coherent chaos shift keying (CSK) and non-coherent differential CSK (DCSK) are popular schemes that have been broadly researched in recent years due to the advantages mentioned above. In the literature, the first study of chaos-based modulation schemes was reported in [29], where permutation-based DCSK and multiple-access DCSK systems were analyzed to enhance data security. In [30], [31], [32], the authors have used the concept of eigen beamforming, space-time coding, and multi-carrier to enhance security of CSK and DCSK schemes. In [28], the anti-synchronization CSK (ACSK) scheme was realized and analyzed using the generalized Lorenz system's anti-synchronization properties. Moreover, it was shown that the resulting ACSK communication scheme has the potential of providing a high degree of security with a low receiver complexity. Furthermore, the PLS performance of CSK and DCSK were evaluated over additive white Gaussian noise and Rayleigh fading channels in [33]. Moreover, generalized correlation delay shift keying (GCDSK) is proposed in [34], where the authors compared the BER performance of the GCDSK with the CDSK scheme and DCSK scheme.

In the past few years, PLC systems have been designed considering many traditional modulation schemes. Meanwhile, the DCSK modulation scheme has been introduced in PLC systems for its robustness. In [25], the performance of DCSK systems over the multipath power line channel model was investigated in the presence of background, impulsive, and phase noise, where the authors concluded that the DCSK schemes perform better than direct sequence differential phase shift keying (DS-DPSK) and the direct sequence code division multiple access

(DS-CDMA) schemes. Similarly, the authors of [35] analyzed the performance of M-ary DCSK (M-DCSK) with background, impulsive, and phase noises, over narrow-band PLC, where it was shown that M-DCSK outperforms direct sequence M-ary differential phase-shift keying (DS-MDPSK). Further, the authors of [35] extended their work in [36] where the replica piecewise (RP)-MDCSK system was designed and studied for PLC with asynchronous impulsive noise. Moreover, the authors demonstrated that RP-MDCSK has a significantly lower bit error rate (BER) than DCSK and DS-MDPSK.

Copulas are novel mathematical functions that provide an easy, flexible, and alternate approach to model correlated multivariate distribution functions in terms of their marginal distributions and mutual dependencies. Copulas have been utilized in statistics, economics, survival analysis, image processing, machine learning, and a wide range of engineering applications [37], [38]. Recently, Copula theory has been explored by researchers in the field of communication channel modeling [39]. Copula-based approaches offer excellent flexibility in mathematical modeling and simplification in computational load compared to the non-Copula-based approaches [40]. In [41], the authors utilized the Copula method to obtain the capacity of a correlated ergodic MIMO channel over Nakagami-*m* fading, where three types of Copulas were used, i.e., normal, Clayton, and *t* Copula for channel parameter estimation. In [39], the authors computed a closed-form expression for the outage probability under cross-correlated Weibull fading using selection combining reception technique by exploiting the survival-Gumbel Copula approach. Similarly, the authors in [42] computed the average symbol error rate and average BER for PLC systems using a quadrature phase shift keying (QPSK) modulation scheme over Nakagami-*m* distributed additive background noise, wherein the Copula approach was used to analyze dependence among decision variables. Furthermore, the authors in [43] utilized the Farlie-Gumbel-Morgenstern (FGM) Copula method to establish the closed-form expressions for the outage probability and coverage region over correlated Rayleigh fading multiple access channels. In [44], the authors analyzed the PLS performance of a correlated Rayleigh distributed wiretap fading channel, where closed-form expressions for the ASC, SOP, and secrecy coverage region (SCR) were derived using the FGM Copula approach.

Motivation: It is important to develop robust, reliable, and trustworthy PLC communication networks for Industry 4.0 and IoT applications. Since PLC technology is broadcast in nature, it becomes crucial to analyze the security of PLC systems for reliable deployment in Industry 4.0 and IoT networks. Contrary to the aforementioned research works [18], [19], [20], [21], [22], where the investigation of the PLS performance of PLC systems is limited to the use of traditional modulation schemes and conventional statistical methods; in this work, we propose a DCSK modulation scheme to investigate the secrecy performance of PLC systems. Furthermore, the correlation between the main PLC channel and the eavesdropper PLC channel is mathematical modeled by exploiting a novel FGM Copula approach. Different from [27], [28], and [32], where it is demonstrated that chaos-based modulation schemes have the ability to provide secure communications against the eavesdropper in wireless communication scenarios; in this work, we employ DCSK modulation in PLC scenarios to analyze the secrecy performance of PLC systems. In contrast to [25], [35], [36], where DCSK modulation was utilized to improve the BER performance of PLC system; in this research, DCSK modulation is utilized to enhance the secrecy performance of PLC systems. Further, contrary to [39], [41], [42], [43], [44], we analyze the PLS performance of a DCSK-based PLC system for correlated Log-normally distributed channels corrupted by additive Bernoulli-Gaussian noise, where the FGM Copula-based approach facilitates the mathematical modeling of PLS performance metrics. We utilize Copula-based methods as they have been empirically proven to provide an easy mathematical modeling and help reduce the computation of jointly distributed multivariate functions [39], [40]. Thus, motivated by the aforementioned works in the literature, we perform the secrecy analysis of a DCSK-based PLC system by exploiting FGM Copula approach.

Contributions: In this work, we investigate the PLS performance of a DCSK-based PLC system by utilizing a novel FGM Copula approach, where a power line Wyners wiretap channel model is analyzed to compute the secrecy between the main channel and the wiretap channel. Both PLC channels are considered to be Log-normally distributed and correlated, and the Bernoulli-Gaussian model characterizes the PLC channel noise. Further, the PLS performance is numerically expressed in terms of SOP and SPSC. To obtain useful insight into the PLC system, the asymptotic SOP analysis is conducted. Furthermore, an algorithm is presented to maximize the secrecy throughput under SOP constraints.

To the best of our knowledge, no previous works have considered Copula theory to investigate the PLS performance of DCSK-based PLC systems. The main contributions of this work are summarized as follows:

- We propose combining the DCSK modulation scheme and FGM Copula approach to investigate the PLS performance of the considered PLC system. The DCSK modulation scheme is utilized to enhance the security of the considered system. Moreover, the FGM Copula approach eases the numerical analysis and shows statistical dependence between the correlated PLC channels.
- To get deep insights into the SOP analysis, the asymptotic behavior of the SOP is investigated, where useful insights, such as diversity order and coding gain of the considered PLC system are revealed. It is shown that the secrecy diversity order depends on the shaping parameter (m_{γ_M}) of the main channel.
- In order to comprehensively investigate the secrecy performance, we formulate an optimization problem

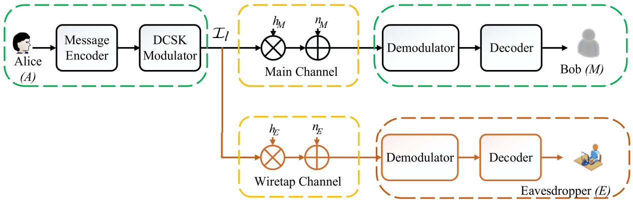

FIGURE 1. Wiretap power line channel system model.

to maximize the secrecy throughput under SOP constraints. We also propose an algorithm to obtain the optimal threshold value of the signal-to-noise ratio (SNR) for SOP.

- We present a comprehensive investigation of the effect of different parameters, such as the spreading factor (β), transmitted power (P_T), impulsive noise occurrence probability (p), and dependence parameter (θ) on the PLS performance metrics of the considered PLC system. We also compare the SOP performance of the proposed system with GCDSK, DS-DPSK, and CDMA. It is found that the proposed system performs better than GCDSK and CDMA for certain values of β.

Organization of the Paper: The rest of the paper is arranged as follows: Section II presents the considered PLC system model, where the DCSK system, received power, PLC channel and noise models, and the characterization of the instantaneous SNR are described. After reviewing Copula theory, the detailed secrecy analysis of the proposed PLC system in terms of SOP and SPSC is presented in Section III. Further, the asymptotic analysis of the SOP is conducted. We also carry out the secrecy throughput optimization analysis in Section III. In Section IV, we demonstrate and discuss the numerical results, while conclusions are drawn in Section V.

Notations: $\mathbb{E}[\cdot]$ denotes the expectation operator, $\mathcal{N}(0, \sigma^2)$ indicates Gaussian distribution with zero mean and variance σ^2, $\Gamma(\cdot)$ is the Gamma function, $\Gamma_l(\cdot, \cdot)$ and $\Gamma_u(\cdot, \cdot)$ represent the lower and upper incomplete Gamma functions, respectively, and ${}_pF_q(\cdot; \cdot; \cdot)$ is the generalized Hypergeometric function.

II. SYSTEM MODEL

Let us consider a discrete memoryless PLC wiretap channel model illustrated in Fig. 1, where Alice (A) transmits a message to an authorized receiver Bob (M) over the main channel. At the same time, a passive eavesdropper (E) wants to listen and attempts to decode the message of A via a wiretap power line channel.

A. DCSK MODULATION

DCSK modulation was recently proposed for PLC systems in [25]. In this modulation, a chaos signal is generated by the chaos generator using a chaotic map. Each signal period is divided into two parts: the first part is assigned to the reference samples and the second part is assigned to the data samples. If the data samples are the same as the reference samples, bit 1 is transmitted, whereas if the data samples are inverted versions of the reference samples, a bit 0 is transmitted. Here, the modulated bits are denoted by $b_i \in \{+1, -1\}$. Let β denote the spreading factor. For the i^{th} bit interval, the modulated output of the DCSK transmitter represented by $\mathcal{I}$, is given as

$$\mathcal{I}_l = \begin{cases} s_l, & 1 < l \leq \beta, \\ b_i s_{l-\beta}, & \beta < l \leq 2\beta, \end{cases} \tag{1}$$

where s_l indicates the chaotic signal used as reference samples and $s_{l-\beta}$ is the delayed version of it. Based on the Gaussian approximation, for large values of β, following assumption can be made [45]

$$\begin{aligned} &\mathbb{E}\Big[s_{i,1}^2 + s_{i,2}^2 + \cdots + s_{i,\beta}^2\Big] \\ &\quad \approx \mathbb{E}\Big[s_{i+1,1+\beta}^2 + s_{i+2,2+\beta}^2 + \cdots + s_{i+\beta,2\beta}^2\Big] \approx 2\beta\mathbb{E}\Big[s_l^2\Big]. \end{aligned} \tag{2}$$

B. RECEIVED POWER

The received signals at M and E are given by

$$r_k = \delta_k \sqrt{P_{R_k}} h_k \mathcal{I}_l + n_k, k \in \{M,\ E\}, \tag{3}$$

where $\delta_k = e^{-(a_0 + a_1 \cdot f^c)d}$ characterizes the attenuation of a power line link and a_0, a_1, and c are the attenuation parameters at a frequency f and path length d. h_M and h_E are the correlated complex channel gains of the main channel and wiretap channel, respectively, which are assumed to undergo flat fading. This is a valid assumption as the considered PLC network has a small number of branches with short lengths (0-300 m), and therefore the signal bandwidth is less than the channel's coherence bandwidth. Consequently, the PLC channels experience flat fading [46], [47]. In Eq. (3), n_M and n_E represent the channel noise on the main channel and eavesdropper channel, respectively, and $\mathcal{I}_l$ denotes the single carrier DCSK modulated symbol transmitted by A.

C. PLC CHANNEL MODEL

For the considered PLC system, we assume that both the main and wiretap channels are Log-normally distributed. The probability density function (PDF) of the PLC channel gain is expressed

$$\begin{aligned} f(|h_k|; \mu_k, \sigma_k) &= \frac{1}{|h_k|\sqrt{2\pi\sigma_k^2}} \exp\left(-\frac{(\ln|h_k| - \mu_k)^2}{2\sigma_k^2}\right), \\ h_k &\geq 0, k \in \{M, E\} \end{aligned} \tag{4}$$

where μ_k and σ_k^2 are the mean and variance of the random variable (RV) $\ln|h_k|$, respectively. Moreover, the channel state information (CSI) of the main and wiretap channels are assumed to be known. In our scenario, it is observed that carrying out the whole analysis with the Log-normal distribution in (4) is quite intractable to obtain the closed-form solution for the double integral expressions. Therefore, we utilize the Gamma approximation of the Log-normal distribution [48, eq. (3)]

$$f(h_k) \approx \frac{1}{\Gamma(m_{h_k})} \left(\frac{m_{h_k}}{\Omega_{h_k}}\right)^{m_{h_k}} h^{m_{h_k}-1} \exp\left(-\frac{m_{h_k} h_k}{\Omega_{h_k}}\right). \tag{5}$$

In (5), the parameters m_{h_k} and Ω_{h_k} hold the following relations with σ_k and μ_k:

$$m_{h_k} = \frac{1}{e^{\sigma_k^2} - 1} \text{ and } \Omega_{h_k} = e^{\mu_k}\sqrt{\frac{m_{h_k}+1}{m_{h_k}}},$$

where $k \in \{M,\ E\}$, m_{h_k} denotes the shaping parameter, and Ω_{h_k} is the mean power.

D. NOISE MODELING

PLC channels generally yield a mixture of background noise and impulsive noise [49], [50]. Background noise occurs due to the addition of all low power noise sources, which can cause disturbance in frequency. Impulsive noise is due to switching transients, which occur all over a power supply network at irregular intervals [51]. The additive noise in a PLC system is usually modeled by the Bernoulli-Gaussian random process [50]. Hence, the total noise can be described by

$$n_k = G'_{n_k} + I_{n_k}, \quad k \in \{M,\ E\} \tag{6a}$$

$$I_{n_k} = P_B G''_{n_k}, \quad k \in \{M,\ E\} \tag{6b}$$

where G'_{n_k} and G''_{n_k} are Gaussian RVs corresponding to the background noise and impulsive noise component of the Bernoulli-Gaussian PLC noise having zero mean and variances σ_B^2 and σ_I^2, respectively. I_{n_k} denotes the impulsive noise, where the Bernoulli RV (P_B) denotes the arrival of impulsive noise component of the PLC noise with the random amplitude of G''_{n_k}. Here, G'_{n_k}, G''_{n_k}, and P_B are assumed to be mutually independent.

Thus, the PDF of the PLC channel noise on the main channel (A to M) and the eavesdropper channel (A to E) is given by [52]

$$f(n_k) = \sum_{j=1}^{2} p_j \mathcal{N}\left(0, \sigma_{k_j}^2\right), k \in \{M,\ E\} \tag{7}$$

where $p_1 = 1 - p$, $p_2 = p$, p is the probability of arrival of the impulsive noise, $\sigma_{k_1}^2 = \sigma_{B_k}^2$ is the background noise power, and $\sigma_{k_2}^2 = \sigma_{B_k}^2(1 + K)$ is the noise power of both background and impulsive noises. $K = \sigma_{I_k}^2/\sigma_{B_k}^2$ denotes the impulsive noise to the background noise power ratio.

E. CHARACTERIZATION OF THE INSTANTANEOUS SNR

The instantaneous SNR of the received DCSK signals at M and E can be written as [52]

$$\gamma_k = \begin{cases} \gamma_{k_1} = \frac{\delta_k^2 |h_k|^2 P_{R_k}}{2\beta\sigma_{B_k}^2} = \mathcal{H}_k \bar{\gamma}_k, & \text{only background noise,} \\ \gamma_{k_2} = \frac{\delta_k^2 |h_k|^2 P_{R_k}}{2\beta\sigma_{B_k}^2(1+K)} = \mathcal{H}_k \bar{\gamma}'_k, & \text{with impulsive noise,} \end{cases} \tag{8}$$

where $k \in \{M,\ E\}$, $\mathcal{H}_k = \delta_k^2|h_k|^2/(2\beta)$, $\bar{\gamma}_k = P_{R_k}/\sigma_{B_k}^2$, and $\bar{\gamma}'_k = \bar{\gamma}_k/(K+1)$. Further, the PDF of γ_{M_j} and γ_{E_j} can be written as

$$f_{\gamma_{k_j}}\left(\gamma_{k_j}\right) = \frac{1}{\Gamma\left(m_{\gamma_{k_j}}\right)}\left(\frac{m_{\gamma_{k_j}}}{\Omega_{\gamma_{k_j}}}\right)^{m_{\gamma_{k_j}}} \gamma^{m_{\gamma_{k_j}}-1} \exp\left(-\frac{m_{\gamma_{k_j}}\gamma_{k_j}}{\Omega_{\gamma_{k_j}}}\right),$$
$$k \in \{M, E\},\ j \in \{1, 2\} \tag{9}$$

where $m_{\gamma_{k_j}} = \frac{1}{e^{\sigma_{\gamma_{k_j}}^2} - 1}$ and $\Omega_{\gamma_{k_j}} = e^{\mu_{\gamma_{k_j}}}\sqrt{\frac{m_{\gamma_{k_j}}+1}{m_{\gamma_{k_j}}}}$. Here, $\mu_{\gamma_{k_1}} = 2\mu_{h_k} + \ln(\delta_k^2/(2\beta)) + \ln\bar{\gamma}_k$, $\mu_{\gamma_{k_2}} = 2\mu_{h_k} + \ln(\delta_k^2/(2\beta)) + \ln\bar{\gamma}'_k$, and $\sigma_{\gamma_{M_j}}^2 = \sigma_{\gamma_{E_j}}^2 = 4\sigma_{h_k}^2$. From (9), the cumulative distribution function (CDF) of γ_{M_j} and γ_{E_j} can be expressed as

$$F_{\gamma_{k_j}}\left(\gamma_{k_j}\right) = \frac{1}{\Gamma\left(m_{\gamma_{k_j}}\right)}\Gamma_l\left(m_{\gamma_{k_j}}, \frac{m_{\gamma_{k_j}}\gamma_{k_j}}{\Omega_{\gamma_{k_j}}}\right). \tag{10}$$

III. PHYSICAL LAYER SECURITY ANALYSIS

A. INTRODUCTION TO COPULA THEORY

Copula functions were first exploited in Mathematics and statistical problems by Sklar [53]. Sklar stated a fundamental theorem for the Copula function, which facilitates the modeling of a correlated multivariate distribution with respect to their marginal distribution functions and a certain mutual dependency. The Sklar's theorem is stated as follows:

Theorem 1 (Sklar's Theroem): Let $F(\alpha_1, \alpha_2, \ldots, \alpha_d)$ be a joint CDF of the RVs defined on $[0, 1]^d$ with their uniform univariate margins $F(\alpha_{d_1})$ for $d_1 = 1, 2, \ldots, d$ over $[0, 1]$. Then, there exists a function in the real domain called Copula function $\mathbb{C}$ defined as

$$F(\alpha_1, \alpha_2, \ldots, \alpha_d) = \mathbb{C}(F(\alpha_1), F(\alpha_2), \ldots, F(\alpha_d)). \tag{11}$$

Using the chain rule in (11), the corresponding joint PDF can be written as

$$\begin{aligned} f(\alpha_1, \alpha_2, \ldots, \alpha_d) &= \frac{\partial^d \mathbb{C}\big(F(\alpha_1), F(\alpha_2), \ldots, F(\alpha_d)\big)}{\partial\alpha_1\partial\alpha_2 \ \ldots \ \partial\alpha_d} \\ &= \frac{\partial^d \mathbb{C}\big(F(\alpha_1), F(\alpha_2), \ldots, F(\alpha_d)\big)}{\partial F(\alpha_1)\partial F(\alpha_2) \ \ldots \ \partial F(\alpha_d)} \times \prod_{d_1=1}^{d} \frac{\partial F\big(\alpha_{d_1}\big)}{\partial\alpha_{d_1}} \\ &= \frac{\partial^d \mathbb{C}\big(F(\alpha_1), F(\alpha_2), \ldots, F(\alpha_d)\big)}{\partial F(\alpha_1)\partial F(\alpha_2) \ \ldots \ \partial F(\alpha_d)} \times \prod_{d_1=1}^{d} f\big(\alpha_{d_1}\big) \\ &= \mathbb{C}_{\mathfrak{f}}\big(F(\alpha_1), F(\alpha_2), \ldots, F(\alpha_d)\big) \times \prod_{d_1=1}^{d} f\big(\alpha_{d_1}\big), \end{aligned} \tag{12}$$

where $\mathbb{C}_{\mathfrak{f}}(F(\alpha_1), F(\alpha_2), \ldots, F(\alpha_d))$ represents the Copula density function and $f(\alpha_{d_1})$ denotes the marginal PDFs.

Various kinds of Copula-based approaches exist, where FGM Copula is particularly popular in many practical applications due to its ability to provide easy and fast computation and to describe the actual dependence between the RVs [40]. In our considered system, the FGM Copula is utilized to analyze the PLS performance metrics. According to the FGM Copula method the joint PDF of γ_{M_j} and γ_{E_j} can be written as

$$f_{\gamma_{M_j},\gamma_{E_j}}(\gamma_{M_j}, \gamma_{E_j}) = f_{\gamma_{M_j}}(\gamma_{M_j}) f_{\gamma_{E_j}}(\gamma_{E_j}) \mathbb{C}_{\mathfrak{f}}(F_{\gamma_{M_j}}(\gamma_{M_j}), F_{\gamma_{E_j}}(\gamma_{E_j})). \tag{13}$$

Further, the FGM Copula function for γ_{M_j} and γ_{E_j} is defined as follows:

$$\begin{aligned}&\mathbb{C}(F\gamma_{M_j}(\gamma_{M_j}), F_{\gamma_{E_j}}(\gamma_{E_j}))\\ &\quad= F_{\gamma_{M_j}}(\gamma_{M_j})F_{\gamma_{E_j}}(\gamma_{E_j})\Big(1+\theta(1-F_{\gamma_{M_j}}(\gamma_{M_j}))(1-F_{\gamma_{E_j}}(\gamma_{E_j}))\Big),\end{aligned} \tag{14}$$

where $\theta \in [-1, 1]$ quantifies the dependency between the RVs γ_{M_j} and γ_{E_j}. A negative dependence between the two RVs is corresponds to $\theta \in [-1, 0)$, $\theta \in (0, 1]$ represents positive dependence between the two RVs, while $\theta = 0$ denotes independence. Taking the partial derivative of (14), the FGM Copula density function can be calculated as

$$\begin{aligned}\mathbb{C}_{\mathfrak{f}}(F_{\gamma_{M_j}}(\gamma_{M_j}), F_{\gamma_{E_j}}(\gamma_{E_j})) &= \frac{\partial^2\mathbb{C}\Big(F_{\gamma_{M_j}}(\gamma_{M_j}), F_{\gamma_{E_j}}(\gamma_{E_j})\Big)}{\partial\gamma_{M_j}\partial\gamma_{E_j}}\\ &= 1+\theta\Big((1-2F_{\gamma_{M_j}}(\gamma_{M_j}))(1-2F_{\gamma_{E_j}}(\gamma_{E_j}))\Big).\end{aligned} \tag{15}$$

Finally, by substituting (15) into (13) and after some mathematical simplifications, the joint PDF of γ_{M_j} and γ_{E_j} can be expressed as

$$\begin{aligned}f_{\gamma_{M_j},\gamma_{E_j}}(\gamma_{M_j},\gamma_{E_j}) &= (1+\theta)f_{\gamma_{M_j}}(\gamma_{M_j})f_{\gamma_{E_j}}(\gamma_{E_j})\\ &\quad-2\theta f_{\gamma_{M_j}}(\gamma_{M_j})f_{\gamma_{E_j}}(\gamma_{E_j})F_{\gamma_{M_j}}(\gamma_{M_j})\\ &\quad-2\theta f_{\gamma_{M_j}}(\gamma_{M_j})f_{\gamma_{E_j}}(\gamma_{E_j})F_{\gamma_{E_j}}(\gamma_{E_j})\\ &\quad+4\theta f_{\gamma_{M_j}}(\gamma_{M_j})f_{\gamma_{E_j}}(\gamma_{E_j})F_{\gamma_{M_j}}(\gamma_{M_j})F_{\gamma_{E_j}}(\gamma_{E_j}).\end{aligned} \tag{16}$$

B. SOP ANALYSIS

The *SOP* is the probability that the instantaneous secrecy capacity falls below a predefined secrecy rate ($\mathrm{R_{th}}$) [54]. By following the same assumption that was mentioned in the work of [55], [56], [57], [58], [59], [60], we have assumed the upper bound on the channel capacity with full knowledge of the noise state available at the transmitter and receivers. Thus, the *SOP* of the considered system can be expressed as [21], [22], [56], [59], [60]

$$SOP = \sum_{j=1}^{2} p_j \times P_{sop_j}, \tag{17}$$

where

$$\begin{aligned}P_{sop_j} &= \left[\Pr\{\mathrm{C}_s(\gamma_{M_j},\gamma_{E_j}) < \mathrm{R_{th}}\}\right] = \left[\Pr\left(\frac{1+\gamma_{M_j}}{1+\gamma_{E_j}} < \exp(\mathrm{R_{th}})\right)\right]\\ &= \left[\Pr\big(\gamma_{M_j} < \lambda\gamma_{E_j}+\lambda-1\big)\right],\end{aligned} \tag{18}$$

where C_s represents the instantaneous secrecy capacity and $\lambda = \exp(\mathrm{R_{th}})$. Further, the exact *SOP* analysis is intractable; due to this, obtaining the closed-form solution of the double integral expressions following (18) becomes quite difficult. Therefore, we proceed with computing the lower bound on *SOP*. In this context, assuming $\lambda(\gamma_{E_j}+1)-1 \approx \lambda\gamma_{E_j}$, we get

$$\begin{aligned}P_{sop_j} &\approx \left[\Pr\{\gamma_{M_j} < \lambda\gamma_{E_j}\}\right]\\ &\approx \int_0^\infty\int_0^{\lambda\gamma_{E_j}} f_{\gamma_{M_j},\gamma_{E_j}}(\gamma_{M_j},\gamma_{E_j})d\gamma_{M_j}d\gamma_{E_j}.\end{aligned} \tag{19}$$

Substituting (16) into (19), we have

$$P_{sop_j} \approx P_{1,j} - P_{2,j} - P_{3,j} + P_{4,j}, \tag{20}$$

where

$$P_{1,j} = (1+\theta)\int_0^\infty\int_0^{\lambda\gamma_{E_j}} f_{M_j}(\gamma_{M_j})f_{E_j}(\gamma_{E_j})d\gamma_{M_j}d\gamma_{E_j}, \tag{21}$$

$$P_{2,j} = 2\theta\int_0^\infty\int_0^{\lambda\gamma_{E_j}} f_{M_j}(\gamma_{M_j})f_{E_j}(\gamma_{E_j})F_{M_j}(\gamma_{M_j})d\gamma_{M_j}d\gamma_{E_j}, \tag{22}$$

$$P_{3,j} = 2\theta\int_0^\infty\int_0^{\lambda\gamma_{E_j}} f_{M_j}(\gamma_{M_j})f_{E_j}(\gamma_{E_j})F_{E_j}(\gamma_{E_j})d\gamma_{M_j}d\gamma_{E_j}, \tag{23}$$

$$P_{4,j} = 4\theta\int_0^\infty\int_0^{\lambda\gamma_{E_j}} f_{M_j}(\gamma_{M_j})f_{E_j}(\gamma_{E_j})F_{M_j}(\gamma_{M_j})F_{E_j}(\gamma_{E_j})d\gamma_{M_j}d\gamma_{E_j}. \tag{24}$$

In **Theorems 2-5**, we derive the series-based expressions for (21)-(24).

Theorem 2: The series-based expressions of $P_{1,j}$ is given as

$$\begin{aligned}P_{1,j} &= \frac{1+\theta}{\Gamma\Big(m_{\gamma_{M_j}}\Big)\Gamma\Big(m_{\gamma_{E_j}}\Big)}\chi^{m_{\gamma_{E_j}}}\left(\frac{\Gamma(\xi)}{m_{\gamma_{M_j}}\eta^{\xi}}\right)\zeta^{m_{\gamma_{M_j}}}\\ &\quad\times {}_2F_1\left(1,\xi;m_{\gamma_{M_j}}+1;\frac{\zeta}{\eta}\right),\end{aligned} \tag{25}$$

where $\chi = (\frac{m_{\gamma_{E_j}}}{\Omega_{\gamma_{E_j}}})$, $\zeta = (\frac{m_{\gamma_{M_j}}\lambda}{\Omega_{\gamma_{M_j}}})$, $\xi = (m_{\gamma_{M_j}} + m_{\gamma_{E_j}})$, and $\eta = (\frac{m_{\gamma_{E_j}}}{\Omega_{\gamma_{E_j}}} + \frac{m_{\gamma_{M_j}}\lambda}{\Omega_{\gamma_{M_j}}})$.

Proof: Refer to Appendix A for the proof. ■

Theorem 3: The series-based expressions of $P_{2,j}$ is expressed as

$$\begin{aligned}P_{2,j} &= \frac{(2\theta)\chi^{m_{\gamma_{E_j}}}}{\Big[\Gamma\Big(m_{\gamma_{M_j}}\Big)\Big]^2\Gamma\Big(m_{\gamma_{E_j}}\Big)}\sum_{\phi=0}^{\infty}\Bigg[\frac{(-1)^\phi}{\phi!\Big(m_{\gamma_{E_j}}+\phi\Big)}\zeta^{\tilde{a}}\\ &\quad\times\left(\frac{\Gamma\Big(\tilde{b}\Big)}{\tilde{a}\eta^{\tilde{b}}}\right){}_2F_1\left(1,\tilde{b};\tilde{a}+1;\frac{\zeta}{\eta}\right)\Bigg],\end{aligned} \tag{26}$$

where $\tilde{b} = (2m_{\gamma_{M_j}} + m_{\gamma_{E_j}} + \phi)$ and $\tilde{a} = (2m_{\gamma_{M_j}} + \phi)$.

Proof: Refer to Appendix B for the proof. ■

Theorem 4: The series-based expressions of $P_{3,j}$ is derived as

$$\begin{aligned}P_{3,j} &= \frac{(2\theta)\zeta^{m_{\gamma_{M_j}}}}{\Gamma\Big(m_{\gamma_{M_j}}\Big)\Big[\Gamma\Big(m_{\gamma_{E_j}}\Big)\Big]^2}\sum_{\phi=0}^{\infty}\Bigg[\frac{(-1)^\phi}{\phi!\Big(m_{\gamma_{E_j}}+\phi\Big)}\chi^{\left(2m_{\gamma_{E_j}}+\phi\right)}\\ &\quad\times\left(\frac{\Gamma\Big(\tilde{d}\Big)}{m_{\gamma_{M_j}}\eta^{\tilde{d}}}\right){}_2F_1\left(1,\tilde{d};m_{\gamma_{M_j}}+1;\frac{\zeta}{\eta}\right)\Bigg],\end{aligned} \tag{27}$$

where $\tilde{d} = (m_{\gamma_{M_j}} + 2m_{\gamma_{E_j}} + \phi)$.

Proof: Refer to Appendix C for the proof. ■

Theorem 5: The series-based expressions of $P_{4,j}$ is given as

$$\begin{aligned}P_{4,j} &= \frac{4\theta}{\Big[\Gamma\Big(m_{\gamma_{M_j}}\Big)\Big]^2\Big[\Gamma\Big(m_{\gamma_{E_j}}\Big)\Big]^2}\sum_{\phi=0}^{\infty}\sum_{\psi=0}^{\infty}\Bigg[\frac{(-1)^\phi}{\phi!\tilde{r}}\frac{(-1)^\psi}{\psi!\tilde{s}}\chi^{\tilde{t}}\\ &\quad\times\left(\frac{\Gamma(\kappa)\zeta^{\tilde{a}}}{\tilde{a}\ \eta^{\kappa}}\right){}_2F_1\left(1,\kappa;\tilde{a}+1;\frac{\zeta}{\eta}\right)\Bigg],\end{aligned} \tag{28}$$

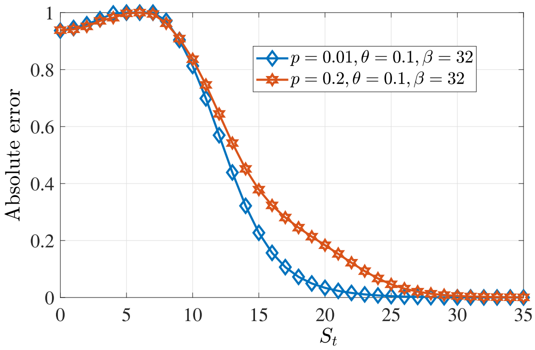

FIGURE 2. Absolute error versus S_t.

where $\tilde{r} = (m_{\gamma_{M_j}} + \phi)$, $\tilde{s} = (m_{\gamma_{E_j}} + \psi)$, $\tilde{t} = (2m_{\gamma_{E_j}} + \psi)$, and $\kappa = (2m_{\gamma_{M_j}} + 2m_{\gamma_{E_j}} + \phi + \psi)$.

Proof: Refer to Appendix D for the proof. ■

C. CONVERGENCE ANALYSIS

On substituting (25)-(28) into (17), the series-based expressions of the *SOP* lower bound is obtained. It is observed from (26)-(28) that the series-based expressions for $P_{2,j}$, $P_{3,j}$, and $P_{4,j}$ consist of infinite summations. Let us present the convergence analysis of the infinite series here. In order to verify the convergence of (17), we calculate the absolute error, defined as

$$\text{Absolute error} = |\text{Exact value Approximated value}|, \quad (29)$$

where the exact value is obtained from (17) and the approximated value is computed from (20) using (25)-(28). Fig. 2 shows the plot of the absolute error against the number of summation terms (S_t) for various values of p, when $\beta = 32, \theta = 0.1, K = 100$, and the transmitted power on the A to M and A to E links is fixed at 20 dB and 10 dB, respectively. It can be noticed from the figure that as the value of S_t increases, the absolute error tends to zero. This demonstrates the convergence of the summation terms in the infinite series of (17). Therefore, in what follows, we consider $S_t = 33$ for our analysis.

D. ASYMPTOTIC SOP ANALYSIS

To gain more insights into the secrecy performance analysis, we analyze the asymptotic behavior of the *SOP* in the high SNR regime. To this end, we start by examining (20) after substituting the series-based expressions of $P_{i,j}$, $i = \{1, 2, 3, 4\}$ from (25)-(28) for high average SNR on the main channel. As $\bar{\gamma}_M \to \infty$, the generalized Hypergeometric function in (25)-(28) tends to unity, i.e., ${}_2F_1(\cdot, \cdot; \cdot; \cdot) \to 1$. The infinite summation vanishes in (26)-(28) because, at high average SNR, only the terms corresponding to $\phi = \psi = 0$ dominate. Hence, the terms $P_{1,j}$, $P_{2,j}$, $P_{3,j}$, and $P_{4,j}$, can be approximated as shown in (30)-(33):

$$P_{1,j} \approx C_{g_{1,j}} \times \left(\frac{1}{\Omega_{\gamma_{M_j}}}\right)^{\overbrace{m_{\gamma_{M_j}}}^{Do_{1,j}}}, \quad (30)$$

$$P_{2,j} \approx C_{g_{2,j}} \times \left(\frac{1}{\Omega_{\gamma_{M_j}}}\right)^{\overbrace{2m_{\gamma_{M_j}}}^{Do_{2,j}}}, \quad (31)$$

$$P_{3,j} \approx C_{g_{3,j}} \times \left(\frac{1}{\Omega_{\gamma_{M_j}}}\right)^{\overbrace{m_{\gamma_{M_j}}}^{Do_{3,j}}}, \quad (32)$$

$$P_{4,j} \approx C_{g_{4,j}} \times \left(\frac{1}{\Omega_{\gamma_{M_j}}}\right)^{\overbrace{2m_{\gamma_{M_j}}}^{Do_{4,j}}}, \quad (33)$$

where

$$C_{g_{1,j}} = \frac{(1+\theta)\chi^{m_{\gamma_{E_j}}}}{\Gamma\left(m_{\gamma_{M_j}}\right)\Gamma\left(m_{\gamma_{E_j}}\right)}\left(\frac{\left(m_{\gamma_{M_j}}\lambda\right)^{m_{\gamma_{M_j}}}\Gamma(\xi)}{m_{\gamma_{M_j}}\chi^{\xi}}\right), \quad (34a)$$

$$C_{g_{2,j}} = \frac{(2\theta)\chi^{m_{\gamma_{E_j}}}}{\left[\Gamma\left(m_{\gamma_{M_j}}\right)\right]^2\Gamma\left(m_{\gamma_{E_j}}\right)}\left(\frac{\left(m_{\gamma_{M_j}}\lambda\right)^{2m_{\gamma_{M_j}}}\Gamma\left(b'\right)}{\left(m_{\gamma_{E_j}}\right)\left(2m_{\gamma_{M_j}}\right)\chi^{b'}}\right), \quad (34b)$$

$$C_{g_{3,j}} = \frac{(2\theta)\chi^{\left(2m_{\gamma_{E_j}}\right)}}{\Gamma\left(m_{\gamma_{M_j}}\right)\left[\Gamma\left(m_{\gamma_{E_j}}\right)\right]^2}\left(\frac{\left(m_{\gamma_{M_j}}\lambda\right)^{m_{\gamma_{M_j}}}\Gamma\left(d'\right)}{\left(m_{\gamma_{E_j}}\right)\left(m_{\gamma_{M_j}}\right)\chi^{d'}}\right), \quad (34c)$$

$$C_{g_{4,j}} = \frac{(2\theta)\chi^{\left(2m_{\gamma_{E_j}}\right)}}{\left[\Gamma\left(m_{\gamma_{M_j}}\right)\right]^2\left[\Gamma\left(m_{\gamma_{E_j}}\right)\right]^2}\left(\frac{\left(m_{\gamma_{M_j}}\lambda\right)^{2m_{\gamma_{M_j}}}\Gamma\left(\kappa'\right)}{\left(m_{\gamma_{E_j}}\right)\left(2m_{\gamma_{M_j}}\right)^2\chi^{\kappa'}}\right). \quad (34d)$$

In (34b), (34c), and (34d), $b' = (2m_{\gamma_{M_j}} + m_{\gamma_{E_j}})$, $d' = (m_{\gamma_{M_j}} + 2m_{\gamma_{E_j}})$, and $\kappa' = (2m_{\gamma_{M_j}} + 2m_{\gamma_{E_j}})$, respectively. Finally, substituting (30)-(33) into (17), the series-based expressions of the asymptotic *SOP* can be computed.

It is known that the asymptotic analysis of any system is characterized by two parameters: coding gain (Cg) and diversity order (Do). The coding gain shows the relative horizontal shift of the *SOP* versus SNR plot on a log-log scale. The diversity order specifies the asymptotic slope of the curve at high SNR values. The relation between coding gain and diversity order for the considered PLC system is computed from (30)-(33) as

$$\lim_{\bar{\gamma}_M \to \infty} SOP \approx \sum_{j=1}^{2} p_j\Bigg[C_{g_{1,j}}\left(\frac{1}{\Omega_{\gamma_{M_j}}(\bar{\gamma}_M)}\right)^{Do_{1,j}} - C_{g_{2,j}}\left(\frac{1}{\Omega_{\gamma_{M_j}}(\bar{\gamma}_M)}\right)^{Do_{2,j}} - C_{g_{3,j}}\left(\frac{1}{\Omega_{\gamma_{M_j}}(\bar{\gamma}_M)}\right)^{Do_{3,j}} + C_{g_{4,j}}\left(\frac{1}{\Omega_{\gamma_{M_j}}(\bar{\gamma}_M)}\right)^{Do_{4,j}}\Bigg]. \quad (35)$$

Furthermore, from (35), the overall diversity order is obtained as $Do = \min\{Do_{1,j}, Do_{2,j}, Do_{3,j}, Do_{4,j}\} = \min\{Do_{1,j}, Do_{3,j}\}$. Thus, (35) can be re-written as

$$\lim_{\bar{\gamma}_M \to \infty} SOP \approx \sum_{j=1}^{2} p_j\left[\underbrace{\left(C_{g_{1,j}} - C_{g_{3,j}}\right)}_{C_{g,j}}\left(\frac{1}{\Omega_{\gamma_{M_j}}(\bar{\gamma}_M)}\right)^{Do_{1,j}}\right], \quad (36)$$

where $Do_{1,j} = Do_{3,j} = m_{\gamma_{M_j}}$.

E. SPSC ANALYSIS

In order to guarantee perfect secrecy over the communication channel, the secrecy capacity must be a non-zero quantity, which is also interpreted as *SPSC*. The *SPSC* for the considered PLC system is given by

$$SPSC = \sum_{j=1}^{2} p_j \times P_{spsc_j}, \tag{37}$$

where

$$\begin{aligned} P_{spsc_j} &= \Pr\left(\gamma_{M_j} > \gamma_{E_j}\right) \\ &= 1 - \Pr\left(\gamma_{M_j} \leq \gamma_{E_j}\right) \\ &= 1 - \int_0^{\infty} \int_0^{\gamma_{E_j}} f_{\gamma_{M_j},\gamma_{E_j}}\left(\gamma_{M_j}, \gamma_{E_j}\right) d\gamma_{M_j} d\gamma_{E_j}. \end{aligned} \tag{38}$$

Here, the integral in (38) can be solved using (16) as

$$P_{spsc_j} = 1 - \left(P'_{1,j} - P'_{2,j} - P'_{3,j} + P'_{4,j}\right), \tag{39}$$

where the series-based expressions for $P'_{1,j}, P'_{2,j}, P'_{3,j}$, and $P'_{4,j}$ can be calculated similar to (25)-(28) by substituting $\lambda = 0$ in (25)-(28) as follows:

$$\begin{aligned} P'_{1,j} = {} & \frac{1+\theta}{\Gamma\left(m_{\gamma_{M_j}}\right)\Gamma\left(m_{\gamma_{E_j}}\right)} \chi^{m_{\gamma_{E_j}}} \left(\frac{\Gamma(\xi)}{m_{\gamma_{M_j}}(\eta')^{\xi}}\right) (\zeta')^{m_{\gamma_{M_j}}} \\ & \times {}_2F_1\left(1, \xi; m_{\gamma_{M_j}}+1; \frac{\zeta'}{\eta'}\right), \end{aligned} \tag{40}$$

$$\begin{aligned} P'_{2,j} = {} & \frac{(2\theta)\chi^{m_{\gamma_{E_j}}}}{\left[\Gamma\left(m_{\gamma_{M_j}}\right)\right]^2 \Gamma\left(m_{\gamma_{E_j}}\right)} \sum_{\phi=0}^{\infty} \left[\frac{(-1)^{\phi}}{\phi!\left(m_{\gamma_{E_j}}+\phi\right)} (\zeta')^{\tilde{a}} \right. \\ & \left. \times \left(\frac{\Gamma\left(\tilde{b}\right)}{\tilde{b}(\eta')^{\tilde{b}}}\right) {}_2F_1\left(1, \tilde{b}; \tilde{a}+1; \frac{\zeta'}{\eta'}\right)\right], \end{aligned} \tag{41}$$

$$\begin{aligned} P'_{3,j} = {} & \frac{(2\theta)(\zeta')^{m_{\gamma_{M_j}}}}{\Gamma\left(m_{\gamma_{M_j}}\right)\left[\Gamma\left(m_{\gamma_{E_j}}\right)\right]^2} \sum_{\phi=0}^{\infty} \left[\frac{(-1)^{\phi}}{\phi!\left(m_{\gamma_{E_j}}+\phi\right)} \chi^{\left(2m_{\gamma_{E_j}}+\phi\right)} \right. \\ & \left. \times \left(\frac{\Gamma\left(\tilde{d}\right)}{m_{\gamma_{M_j}}(\eta')^{\tilde{d}}}\right) {}_2F_1\left(1, \tilde{d}; m_{\gamma_{M_j}}+1; \frac{\zeta'}{\eta'}\right)\right], \end{aligned} \tag{42}$$

$$\begin{aligned} P'_{4,j} = {} & \frac{4\theta}{\Gamma\left(m_{\gamma_{M_j}}\right)^2 \Gamma\left(m_{\gamma_{E_j}}\right)^2} \sum_{\phi=0}^{\infty}\sum_{\psi=0}^{\infty} \left[\frac{(-1)^{\phi}}{\phi!\tilde{r}} \frac{(-1)^{\psi}}{\psi!\tilde{s}} \chi^{\tilde{t}} \right. \\ & \left. \times \left(\frac{\Gamma(\kappa)(\zeta')^{\tilde{a}}}{\tilde{a}(\eta')^{\kappa}}\right) {}_2F_1\left(1, \kappa; \tilde{a}+1; \frac{\zeta'}{\eta'}\right)\right], \end{aligned} \tag{43}$$

where $\zeta' = \left(\frac{m_{\gamma_{M_j}}}{\Omega_{\gamma_{M_j}}}\right)$ and $\eta' = \left(\frac{m_{\gamma_{E_j}}}{\Omega_{\gamma_{E_j}}} + \frac{m_{\gamma_{M_j}}}{\Omega_{\gamma_{M_j}}}\right)$.

F. SECRECY THROUGHPUT OPTIMIZATION ANALYSIS

In this section, we consider the secrecy throughput optimization for the considered PLC system. Our objective is to maximize the secrecy throughput under the *SOP* constraints; an algorithm is proposed for the same in this subsection.

Let us assume the Wyner's wiretap encoding scheme for the considered system model, where A transmits information at rate R_M to M by maintaining a predefined secrecy rate R_{th} against E. The net rate difference $\mathrm{R}_D = \mathrm{R}_M - \mathrm{R}_{\text{th}}$ estimates the cost of securing data transmission. For perfect secrecy, the main channel (A to M link) must follow the condition $\mathrm{C}_M > \mathrm{R}_{\text{th}}$. Otherwise, perfect secrecy fails, i.e., $\mathrm{C}_E > \mathrm{R}_D$, where C_M and C_E are the instantaneous channel capacities of M and E, respectively. Thus, the conditional *SOP* is formulated as [61]

$$P_{csop_j} \triangleq \Pr\left(\mathrm{C}_{E_j} > \mathrm{R}_{M_j} - \mathrm{R}_{\text{th}} | \text{ data transmission}\right). \tag{44}$$

Using (44), the overall conditional *SOP* of the considered system can be written as

$$CSOP = \sum_{j=1}^{2} p_j \times P_{csop_j}. \tag{45}$$

We aim to maximize the secrecy throughput for the considered PLC system. The secrecy throughput is defined as

$$\tau = P_{\text{tx}} \mathrm{R}_{\text{th}}, \tag{46}$$

where P_{tx} denotes the transmission probability. Hence, the optimization problem can be formulated as

$$\max\ \tau, \quad \text{s.t. } CSOP \leq \rho,\ P_{\text{tx}} \geq \nu, \tag{47}$$

where $\rho \in [0, 1]$ and $\nu \in [0, 1]$ represent the constraints for secure and reliable transmission, respectively. In addition, we assume that the data transmission is possible whenever the value of γ_M is greater than a certain threshold SNR, γ_{th}, with $\gamma_{\text{th}} \geq \exp(\mathrm{R}_{\text{th}}) - 1$. Therefore, the transmission probability can be expressed as

$$\begin{aligned} P_{\text{tx}} &= \Pr\left(\gamma_{M_j} > \gamma_{\text{th}}\right) = \frac{1}{\Gamma\left(m_{\gamma_{M_j}}\right)} \Gamma_u\left(m_{\gamma_{M_j}}, \frac{m_{\gamma_{M_j}}\gamma_{\text{th}}}{\Omega_{\gamma_{M_j}}}\right) \\ &= \frac{1}{\Gamma\left(m_{\gamma_{M_j}}\right)}\left[\Gamma\left(m_{\gamma_{M_j}}\right) - \sum_{i=0}^{\infty} \frac{(-1)^i}{i!\left(m_{\gamma_{M_j}}+i\right)} \left(\frac{m_{\gamma_{M_j}}\gamma_{\text{th}}}{\Omega_{\gamma_{M_j}}}\right)^{m_{\gamma_{M_j}}+i}\right]. \end{aligned} \tag{48}$$

Let us evaluate the conditional *SOP* as follows:

$$\begin{aligned} P_{csop_j} &= \Pr\left(\mathrm{C}_{E_j} > \mathrm{C}_{M_j} | \gamma_{M_j} > \gamma_{\text{th}}\right) \\ &= \Pr\left(\gamma_{M_j} < \exp(\mathrm{R}_{\text{th}})\left(1+\gamma_{E_j}\right) - 1 | \gamma_{M_j} > \gamma_{\text{th}}\right) \\ &= \frac{\Pr\left(\gamma_{\text{th}} < \gamma_{M_j} < \lambda\left(1+\gamma_{E_j}\right) - 1\right)}{\Pr\left(\gamma_{M_j} > \gamma_{\text{th}}\right)}. \end{aligned} \tag{49}$$

Considering the lower bound in (49), i.e., $\lambda(\gamma_{E_j}+1) - 1 \approx \lambda\gamma_{E_j}$, we obtain

$$\begin{aligned} P_{csop_j} &\approx \frac{\Pr\left(\gamma_{\text{th}} < \gamma_{M_j} < \lambda\gamma_{E_j}\right)}{\Pr\left(\gamma_{M_j} > \gamma_{\text{th}}\right)} \\ &\approx \frac{\int_{\Theta}^{\infty} \int_{\gamma_{\text{th}}}^{\lambda\gamma_{E_j}} f_{\gamma_{M_j},\gamma_{E_j}}\left(\gamma_{M_j}, \gamma_{E_j}\right) d\gamma_{M_j} d\gamma_{E_j}}{\Pr\left(\gamma_{M_j} > \gamma_{\text{th}}\right)}, \end{aligned} \tag{50}$$

where $\Theta = (\frac{1+\gamma_{\text{th}}}{\lambda}) - 1$. Here, the double integral in (50) can be divided into two parts as follows:

$$\mathbb{I} = \underbrace{\int_{\Theta}^{\infty}\int_{0}^{\lambda\gamma_{E_j}} f_{\gamma_{M_j},\gamma_{E_j}}\left(\gamma_{M_j},\gamma_{E_j}\right) d\gamma_{M_j} d\gamma_{E_j}}_{I_{1,j}} - \underbrace{\int_{\Theta}^{\infty}\int_{0}^{\gamma_{\text{th}}} f_{\gamma_{M_j},\gamma_{E_j}}\left(\gamma_{M_j},\gamma_{E_j}\right) d\gamma_{M_j} d\gamma_{E_j}}_{I_{2,j}}. \tag{51}$$

By substituting (17) into (38), we get $I_{1,j} \approx I_{11,j} - I_{12,j} - I_{13,j} + I_{14,j}$ and $I_{2,j} \approx I_{21,j} - I_{22,j} - I_{23,j} + I_{24,j}$. The series-based expressions for $I_{1i,j}$, $i = \{1, 2, 3, 4\}$ can be obtained following a similar approach to (21)-(24) as

$$I_{11,j} \approx \frac{(1+\theta)(\chi\lambda)^{m_{\gamma_{E_j}}}}{\left[\Gamma\left(m_{\gamma_{M_j}}\right)\right]^2 \Gamma\left(m_{\gamma_{E_j}}\right)} \sum_{\phi=0}^{\infty} \frac{(-1)^{\phi}\zeta^{\tilde{r}}}{\phi\tilde{r}} \times \left[\Gamma(\xi+\phi) - \sum_{\psi=0}^{\infty} \frac{(-1)^{\psi}}{\psi!(\xi+\phi+\psi)} \left(\zeta'\Theta\right)^{\xi+\phi+\psi}\right], \tag{52}$$

$$I_{12,j} \approx \frac{2\theta}{\left[\Gamma\left(m_{\gamma_{M_j}}\right)\right]^2 \Gamma\left(m_{\gamma_{E_j}}\right)} \sum_{\phi=0}^{\infty}\sum_{\psi=0}^{\infty} \frac{(-1)^{\phi}}{\phi!\tilde{r}} \frac{(-1)^{\psi}}{\psi!(\tilde{a}+\psi)} \times (\zeta)^{\tilde{a}+\psi} \left[\Gamma\left(\tilde{b}+\psi\right) - \sum_{\varphi=0}^{\infty} \frac{(-1)^{\varphi}(\chi\Theta)^{\tilde{b}+\psi+\varphi}}{\varphi!\left(\tilde{b}+\psi+\varphi\right)}\right], \tag{53}$$

$$I_{13,j} \approx \frac{2\theta}{\left[\Gamma\left(m_{\gamma_{M_j}}\right)\right]^2 \left[\Gamma\left(m_{\gamma_{E_j}}\right)\right]^2} \sum_{\phi=0}^{\infty}\sum_{\psi=0}^{\infty} \frac{(-1)^{\phi}\zeta^{\tilde{r}}}{\phi!\tilde{r}} \chi^{\tilde{t}} \times \frac{(-1)^{\psi}}{\psi!\tilde{s}} \left[\Gamma(\xi+\phi) - \sum_{\varphi=0}^{\infty} \frac{(-1)^{\varphi}(\chi\Theta)^{\xi+\phi+\varphi}}{\varphi!(\xi+\phi+\varphi)}\right], \tag{54}$$

$$I_{14,j} \approx \frac{2\theta}{\left[\Gamma\left(m_{\gamma_{M_j}}\right)\right]^3 \left[\Gamma\left(m_{\gamma_{E_j}}\right)\right]^2} \sum_{\phi=0}^{\infty}\sum_{\psi=0}^{\infty}\sum_{\varphi=0}^{\infty} \frac{(-1)^{\phi}}{\phi!\tilde{r}} \frac{(-1)^{\psi}}{\psi!\tilde{s}} \times (\zeta)^{\tilde{a}+\varphi} \frac{(-1)^{\varphi}\chi^{\tilde{t}}}{\varphi!(\tilde{a}+\varphi)} \left[\Gamma(\kappa+\varphi+\omega) - \sum_{\omega=0}^{\infty} \frac{(-1)^{\omega}(\chi\Theta)^{\kappa+\varphi+\omega}}{\omega!(\kappa+\varphi+\omega)}\right]. \tag{55}$$

Likewise, the series-based expressions for $I_{2i,j}$, $i = \{1, 2, 3, 4\}$ is obtained as

$$I_{21,j} \approx \frac{1+\theta}{\left[\Gamma\left(m_{\gamma_{M_j}}\right)\right]^2 \Gamma\left(m_{\gamma_{E_j}}\right)} \sum_{\phi=0}^{\infty} \frac{(-1)^{\phi}\left(\zeta'\gamma_{\text{th}}\right)^{\tilde{r}}}{\phi!\tilde{r}} \times \left[\Gamma\left(m_{\gamma_{E_j}}\right) - \sum_{\psi=0}^{\infty} \frac{(-1)^{\psi}}{\psi!\tilde{s}} (\chi\Theta)^{\tilde{s}}\right], \tag{56}$$

$$I_{22,j} \approx \frac{(2\theta)\chi^{\left(m_{\gamma_{E_j}}\right)}}{\left[\Gamma\left(m_{\gamma_{M_j}}\right)\right]^3 \left[\Gamma\left(m_{\gamma_{E_j}}\right)\right]^2} \sum_{\phi=0}^{\infty}\sum_{\psi=0}^{\infty} \frac{(-1)^{\phi}}{\phi!\tilde{r}} \frac{(-1)^{\psi}}{\psi!(\tilde{a}+\psi)} \times \left(\zeta'\gamma_{\text{th}}\right)^{\tilde{a}+\psi} \left[\Gamma\left(m_{\gamma_{E_j}}\right) - \sum_{\varphi=0}^{\infty} \frac{(-1)^{\varphi}}{\varphi!\left(m_{\gamma_{E_j}}+\varphi\right)} (\chi\Theta)^{m_{\gamma_{E_j}}+\varphi}\right], \tag{57}$$

$$I_{23,j} \approx \frac{2\theta}{\left[\Gamma\left(m_{\gamma_{M_j}}\right)\right]^2 \left[\Gamma\left(m_{\gamma_{E_j}}\right)\right]^3} \sum_{\phi=0}^{\infty}\sum_{\psi=0}^{\infty} \frac{(-1)^{\phi}}{\phi!\tilde{r}} \frac{(-1)^{\psi}}{\psi!\tilde{s}} \times \left(\zeta'\gamma_{\text{th}}\right)^{\tilde{r}} \left[\Gamma(\tilde{t}) - \sum_{\varphi=0}^{\infty} \frac{(-1)^{\varphi}}{\varphi!(\tilde{t}+\varphi)} (\chi\Theta)^{\tilde{t}+\varphi}\right], \tag{58}$$

Algorithm 1: Algorithm for Finding the Optimal γ_{th} to Maximize the Secrecy Throughput

```
Initialization: $R_{th}$, $\rho$, and $\nu$;
Optimization problem given in (47) and obtain CSOP and $P_{tx}$ given in (45) and (48), respectively;
To maximize $\tau$, we aim to find the optimal value of $\gamma_{th}$ for the considered design problem given in (60a) to (60c);
do
    Calculate $\gamma_{th}$ by (48)
while $P_{tx}(\gamma_{th}) \geq \nu$, $\gamma_{th} \geq \exp(R_{th}) - 1$, and $R_{th} > 0$;
Find optimal value of $\gamma_{th}$;
do
    Calculate $\gamma_{th}$ using expression $CSOP(\gamma_{th}, R_{th}) = \rho$
while $CSOP(\gamma_{th}, R_{th}) \leq \rho$;
Finally, a feasible range of optimal $\gamma_{th}$ is given by (61);
```

$$I_{24,j} \approx \frac{2\theta}{\left[\Gamma\left(m_{\gamma_{M_j}}\right)\right]^3 \left[\Gamma\left(m_{\gamma_{E_j}}\right)\right]^3} \sum_{\phi=0}^{\infty}\sum_{\psi=0}^{\infty}\sum_{\varphi=0}^{\infty} \frac{(-1)^{\phi}}{\phi!\tilde{r}} \frac{(-1)^{\psi}}{\psi!\tilde{s}} \times \frac{(-1)^{\varphi}\left(\zeta'\gamma_{\text{th}}\right)^{\tilde{a}+\varphi}}{\varphi!(\tilde{a}+\varphi)} \left[\Gamma\left(2m_{\gamma_{M_j}}+\psi\right) - \sum_{\omega=0}^{\infty} \frac{(-1)^{\omega}}{\omega!\tilde{q}} (\chi\Theta)^{\tilde{q}}\right], \tag{59}$$

where $\tilde{q} = (2m_{\gamma_{M_j}} + 2m_{\gamma_{E_j}} + \psi + \omega)$. Finally, substituting (52)-(59) into (45), the series-based expressions of *CSOP* can be obtained. Now, to maximize the secrecy throughput, we find the optimal value of γ_{th} for the considered optimization problem as follows:

$$\arg\max_{\gamma_{\text{th}}} \; P_{\text{tx}}(\gamma_{\text{th}})\mathrm{R}_{\text{th}}, \tag{60a}$$

$$\text{s.t.} \; CSOP(\gamma_{\text{th}}, \mathrm{R}_{\text{th}}) \leq \rho, \quad P_{\text{tx}}(\gamma_{\text{th}}) \geq \nu, \tag{60b}$$

$$\gamma_{\text{th}} \geq \exp(\mathrm{R}_{\text{th}}) - 1, \quad \mathrm{R}_{\text{th}} > 0, \tag{60c}$$

where P_{tx} and *CSOP* are the function of γ_{th} and R_{th}. Therefore, using (48) the possible range of γ_{th} is obtained by following $P_{\text{tx}}(\gamma_{\text{th}}) \geq \nu$. Thus, $\gamma_{\text{th}} \in [\exp(\mathrm{R}_{\text{th}}) - 1, \gamma_{\text{th,u}}]$, where $\gamma_{\text{th,u}}$ is the upper limit of γ_{th} computed from (48). Herein, to maximize the secrecy throughput the smallest value of γ_{th} is considered whilst satisfying security constraints. Since, (45) is a decreasing function of γ_{th}, the optimal γ_{th} can be obtained using $CSOP(\gamma_{\text{th}}, \mathrm{R}_{\text{th}}) = \rho$, by following $CSOP(\gamma_{\text{th}}, \mathrm{R}_{\text{th}}) \leq \rho$, as

$$\gamma_{\text{th}} = \begin{cases} \exp(R_{\text{th}}) - 1, & \text{if } \mathrm{R}_{\text{th}} \leq \ln \frac{\bar{\gamma}_M \rho}{\bar{\gamma}_E (1-\rho)}, \\ \gamma_{\text{th,u}'}, & \text{otherwise}, \end{cases} \tag{61}$$

where $\gamma_{\text{th,u}'}$ represents the upper limit of γ_{th}. It should be noted that the optimal value of γ_{th} given by (45) and (48) is calculated using MATLAB software for mathematical tractability. The algorithm to compute the optimal value of γ_{th} that maximizes the secrecy throughput is summarized as the algorithm 1.

IV. NUMERICAL RESULTS AND DISCUSSION

In this section, numerical results and discussion are presented to analyze the performance of the proposed system. The analytical plots are obtained using the derived theoretical

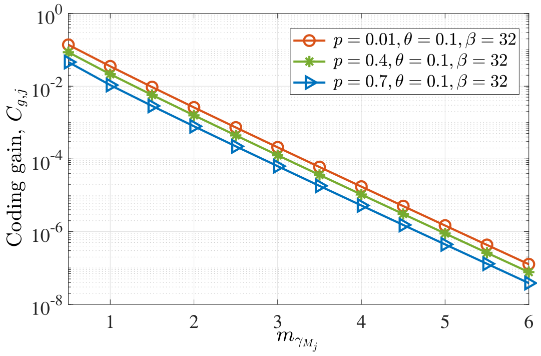

FIGURE 3. Plot of coding gain versus $m_{\gamma_{M_j}}$.

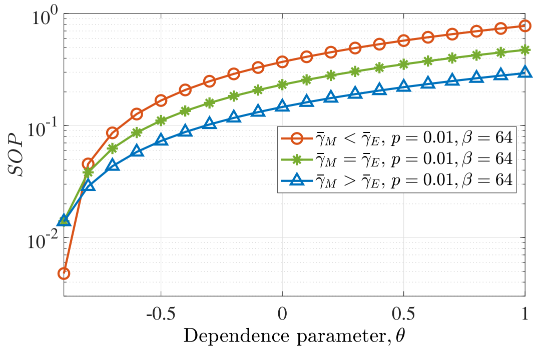

FIGURE 5. ***SOP*** **versus θ for different $\bar{\gamma}_M$ and $\bar{\gamma}_E$, when $p = 0.01$ and $\beta = 64$.**

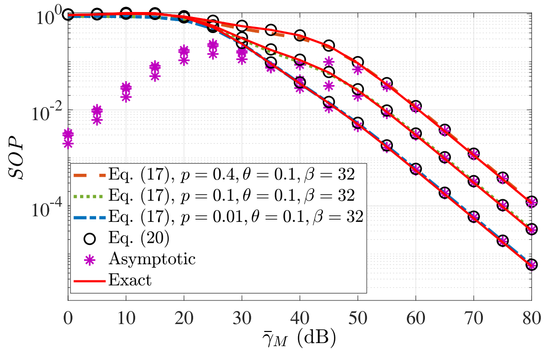

FIGURE 4. **Comparison of *SOP* versus $\bar{\gamma}_M$ for various values of p, when $\theta = 0.1$, $\beta = 32$, and $K = 100$.**

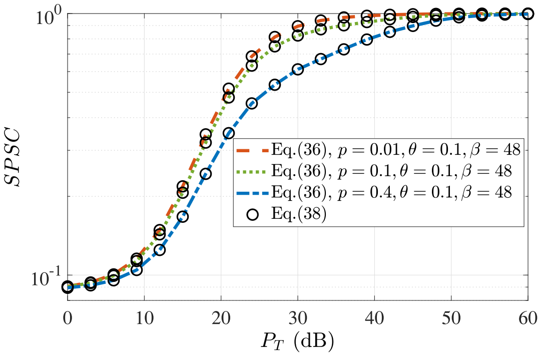

FIGURE 6. ***SPSC*** **versus P_T for various values of p, when $\theta = 0.1$, $\beta = 48$, and $K = 100$.**

results. We assume that the frequency is 1 MHz and the distance from A to M and from A to E is set to 300 m. Moreover, $a_0 = 8.40 \times 10^{-3}$ m^{-1}, $a_1 = 3 \times 10^{-9}$ s/m, and $c = 1$.

In Fig. 3, we plot the coding gain as a function of the diversity order for various values of p, when $\theta = 0.1$, $\beta = 32$, $K = 100$, and the transmitted power on the A to M and the A to E links are 20 dB and 10 dB, respectively. It can be observed from the figure that as the secrecy diversity order $m_{\gamma_{M_j}}$ increases, the overall $C_{g,j}$ decreases. Moreover, the $C_{g,j}$ improves as the value of p is reduced from 0.7 to 0.01.

Fig. 4 illustrates the *SOP* versus $\bar{\gamma}_M$ curves for various values of p, when $\theta = 0.1$, $\beta = 32$, $K = 100$, and transmitted power on the A to E link is fixed at 20 dB. It is explicitly shown in the figure that the *SOP* performance is better for lower values of p and increasing p degrades the *SOP*. This is because the frequent occurrence of impulsive noise causes, the PLC system's overall noise power to increase, which negatively affects the *SOP* performance of the considered system. Moreover, it is observed that the lower bound *SOP* curves are very close to the exact *SOP* curves, which is the accuracy of the derived *SOP* lower bound. Additionally, the asymptotic *SOP* as a function of the average SNR is shown in Fig. 4. Here, the *SOP* is 5.97×10^{-5} and 5.97×10^{-6} at 70 dB and 80 dB, respectively, for $p = 0.01$, $\theta = 0.1$, $\beta = 32$, and the transmitted power on the A to E link is fixed at 20 dB. Therefore, the asymptotic slope is computed as $\log_{10}(5.97 \times 10^{-5}) - \log_{10}(5.97 \times 10^{-6}) = 1 = \min\{m_{\gamma_{M_j}}, 2m_{\gamma_{M_j}}\}$, which is in line with the asymptotic slope theoretically calculated in (35).

In Fig. 5, the *SOP* is plotted as a function of the dependence parameter θ for $p = 0.01$ and $\beta = 64$ under different SNR conditions ($\bar{\gamma}_M > \bar{\gamma}_E$, $\bar{\gamma}_M = \bar{\gamma}_E$, and $\bar{\gamma}_M < \bar{\gamma}_E$). When $\bar{\gamma}_M < \bar{\gamma}_E$, the *SOP* performance deteriorates with increasing θ compared to the other two conditions. Receiving a high SNR at E increases its channel capacity, which implies higher chances of secrecy outage. Therefore, the PLC channel becomes less secure. Similarly, when $\bar{\gamma}_M > \bar{\gamma}_E$ the *SOP* performance is improved. This is because receiving a high SNR at M increases the capacity of the main PLC channel. As a result, there are less chance of an outage. Finally, for $\bar{\gamma}_M = \bar{\gamma}_E$ the *SOP* performance is moderate. In all the three conditions, it is revealed that as θ increases to 1, the *SOP* also tends to 1. This observation is quite intuitive because high positive values of θ indicate higher dependency between the main channel and the eavesdropper channel, thereby making the PLC transmission less secure.

Fig. 6 shows the *SPSC* versus the transmitted power on the A to M link for various values of p, when $\theta = 0.1$, $\beta = 48$, and $K = 100$, under a fixed transmitted power of 20 dB on the A to E link. It is clearly shown in the figure

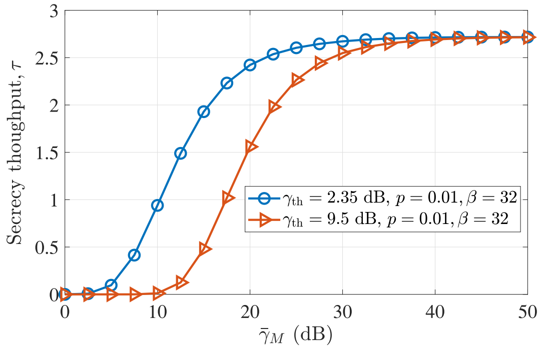

FIGURE 7. Secrecy throughput versus $\bar{\gamma}_M$ for various values of γ_{th}, when $p = 0.01$, $\beta = 32$, and $K = 100$.

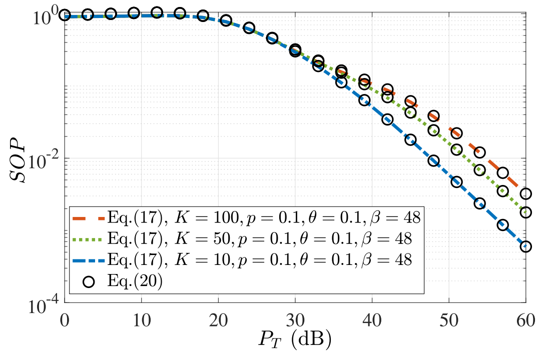

FIGURE 8. *SOP* versus P_T plot for different values of K, when $p = 0.1$, $\theta = 0.1$, and $\beta = 48$.

that the *SPSC* performance improves as the value of p is reduced from 0.4 to 0.05.

Fig. 7 depicts the secrecy throughput versus $\bar{\gamma}_M$ for different values of γ_{th}, when $p = 0.01$, $\beta = 32$, $K = 100$, $\text{R}_{\text{th}} = 1$, and $\bar{\gamma}_E = 0$ dB. Herein, $\gamma_{\text{th}} = 2.35$ dB is obtained by $\gamma_{\text{th}} = \exp(\text{R}_{\text{th}}) - 1$. Likewise, $\gamma_{\text{th}} = 9.5$ dB is computed assuming $CSOP(\gamma_{\text{th}}, \text{R}_{\text{th}}) = \rho$ for $p = 0.01$, $\beta = 32$, $\rho = 0.2$, and $\theta = 0.1$, when the transmitted power on the A to M and the A to E links fixed at 20 dB and 8 dB, respectively. It is observed that secrecy throughput improves with a lower value of γ_{th} because there are less chances of outage for lower values of γ_{th}. Similarly, there is a high outage probability for high values of γ_{th}, and therefore the secrecy throughput decreases with the increase of γ_{th}. It is noted that, the computed values of γ_{th} that maximize the secrecy throughput satisfy all the optimization conditions given in (60b) and (60c). For instance, it is observed from the figure that when $\gamma_{\text{th}} = 9.5$ dB, $CSOP = 0.134$ and $P_{\text{tx}} = 0.987$ for $\rho = 0.2$ and $\nu = 0.4$, which satisfy the optimization conditions in (60b) and (60c).

The *SOP* of the considered PLC system as a function of transmitted power on the A to M link for different values of K is shown in Fig. 8. The curves are plotted for $p = 0.1, \theta = 0.1$, $\beta = 48$, and the transmitted power of the A to E link is fixed at 20 dB. It is observed that the *SOP* performance degrades as the value of K increases. Moreover, it is inferred from the plot that the value of the impulsive noise index parameter severely affect the behavior of the proposed PLC communication system.

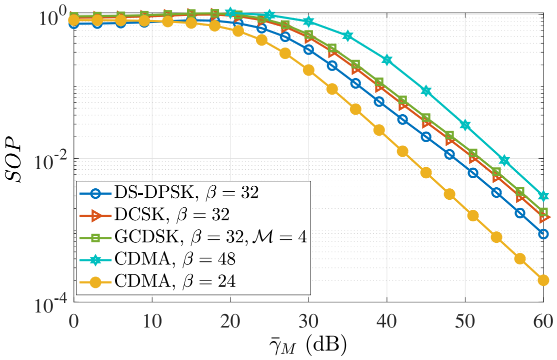

FIGURE 9. *SOP* versus $\bar{\gamma}_M$ for different modulation schemes, when $\beta = 24, 32, 48$, and $\mathcal{M} = 4$.

Fig. 9 shows the comparison of *SOP* as a function of $\bar{\gamma}_M$ for the different modulation schemes such as DCSK, DS-DPSK, GCDSK, and CDMA. It is found that the SOP performance of DCSK is superior to GCDSK for selected values of β and delay block ($\mathcal{M}$). Additionally, the GCDSK system structure is complex and complicated. It requires an additional delay, correlator, and multiplier [35]. However, CDMA performs worse with a higher value of β and vice-versa. Further, it is noticed that the SOP performance of DS-DPSK is better than DCSK. However, the DCSK system inherits chaos signal properties that make the interception and decoding of data more difficult for an eavesdropper.

V. CONCLUSION

In this paper, we investigated the secrecy performance of DCSK-based PLC systems under correlated Log-normally distributed PLC wiretap channel. The FGM Copula approach facilitated the mathematical modeling of the PLS performance metrics in terms of *SOP* and *SPSC*. Specifically, the FGM Copula explicitly shows the correlation between the main and the wiretap channels in terms of the dependence parameter. In addition, to further understand the PLC system performance the asymptotic analysis was carried out, where a relation was established between the secrecy coding gain and the secrecy diversity order. We also presented an algorithm to maximize the secrecy throughout under *SOP* constraints. The algorithm is used to find the optimal SNR for which secrecy throughput is maximum. Useful insights into the considered PLC system were ascertained by studying the impact of different parameters such as the spreading factor, impulsive noise occurrence probability, transmitted power, dependence parameter, and impulsive noise index.

APPENDIX A
PROOF OF THEOREM 2

By substituting (9) and (10) into (21), we obtain

$$P_{1,j} = \frac{(1+\theta)\chi^{m_{\gamma_{E_j}}} \left(\zeta'\right)^{m_{\gamma_{M_j}}}}{\Gamma\left(m_{\gamma_{M_j}}\right)\Gamma\left(m_{\gamma_{E_j}}\right)} \int_0^\infty I_{3,j} \times \gamma^{m_{\gamma_{E_j}}-1} \exp\left(\chi \gamma_{E_j}\right) d\gamma_{E_j}. \tag{62}$$

From [62, eq. (3.381.3)], the inner integral $I_{3,j}$ can be solved as

$$I_{3,j} = \int_0^{\gamma_{E_j}\lambda} \gamma_{k_j}^{m_{\gamma_{k_j}}-1} \exp\left(\zeta' \gamma_{M_j}\right) d\gamma_{M_j} = \frac{1}{\Gamma\left(m_{\gamma_{M_j}}\right)} \Gamma_l\left(m_{\gamma_{M_j}}, \zeta \gamma_{E_j}\right). \tag{63}$$

Thus, substituting (63) into (62) and using [62, Eq. (6.455.2)] in the ensuing integral, the series-based expressions for $P_{1,j}$ is obtained as (25) in **Theorem 2**.

APPENDIX B PROOF OF THEOREM 3

By substituting (9) and (10) into (22), we get

$$P_{2,j} = \frac{(2\theta)\chi^{m_{\gamma_{E_j}}}\left(\zeta'\right)^{m_{\gamma_{M_j}}}}{\left[\Gamma\left(m_{\gamma_{M_j}}\right)\right]^2 \Gamma\left(m_{\gamma_{E_j}}\right)} \int_0^\infty I_{3,j} \times \gamma^{m_{\gamma_{E_j}}-1} \exp\left(\chi \gamma_{E_j}\right) \times \Gamma_l\left(m_{\gamma_{M_j}}, \zeta' \gamma_{M_j}\right) d\gamma_{E_j}, \tag{64}$$

where the incomplete lower Gamma function can be approximated [62, eq. (3.381.2)] as

$$\Gamma_l\left(m_{\gamma_{M_j}}, \zeta' \gamma_{M_j}\right) = \sum_{\phi=0}^{\infty} \frac{(-1)^\phi}{\phi!\left(m_{\gamma_{M_j}} + \phi\right)} \left(\zeta' \gamma_{M_j}\right)^{m_{\gamma_{M_j}}+\phi}. \tag{65}$$

Thus, substituting (63) into (64) and utilizing [62, eq. (6.455.2)] in the ensuing integral, the series-based expressions for $P_{2,j}$ is obtained as (26) in **Theorem 3**.

APPENDIX C PROOF OF THEOREM 4

By substituting (9) and (10) into (23), we get

$$P_{3,j} = \frac{(2\theta)\chi^{m_{\gamma_{E_j}}}\left(\zeta'\right)^{m_{\gamma_{M_j}}}}{\Gamma\left(m_{\gamma_{M_j}}\right)\left[\Gamma\left(m_{\gamma_{E_j}}\right)\right]^2} \int_0^\infty I_{3,j} \times \gamma^{m_{\gamma_{E_j}}-1} \exp\left(\chi \gamma_{E_j}\right) \times \Gamma_l\left(m_{\gamma_{E_j}}, \chi \gamma_{E_j}\right) d\gamma_{E_j}, \tag{66}$$

where the incomplete lower Gamma function can be approximated [62, eq. (3.381.2)] as

$$\Gamma_l\left(m_{\gamma_{E_j}}, \chi \gamma_{E_j}\right) = \sum_{\psi=0}^{\infty} \frac{(-1)^\psi}{\psi!\left(m_{\gamma_{E_j}} + \psi\right)} \left(\chi \gamma_{E_j}\right)^{m_{\gamma_{E_j}}+\psi}. \tag{67}$$

Thus, substituting (63) into (66) and utilizing [62, eq. (6.455.2)] in the ensuing integral, the series-based expressions for $P_{3,j}$ is derived as (27) in **Theorem 4**.

APPENDIX D PROOF OF THEOREM 5

By substituting (9) and (10) into (24), we get

$$P_{3,j} = \frac{(2\theta)\chi^{m_{\gamma_{E_j}}}\left(\zeta'\right)^{m_{\gamma_{M_j}}}}{\left[\Gamma\left(m_{\gamma_{M_j}}\right)\right]^2\left[\Gamma\left(m_{\gamma_{E_j}}\right)\right]^2} \int_0^\infty I_{3,j} \times \gamma^{m_{\gamma_{E_j}}-1} \exp\left(\chi \gamma_{E_j}\right) \times \Gamma_l\left(m_{\gamma_{M_j}}, \zeta' \gamma_{M_j}\right) \Gamma_l\left(m_{\gamma_{E_j}}, \chi \gamma_{E_j}\right) d\gamma_{E_j}. \tag{68}$$

Thus, substituting (63), (65), and (67) into (68) and utilizing [62, eq. (6.455.2)] in the ensuing integral, the series-based expressions for $P_{4,j}$ is derived as (28) in **Theorem 5**.

REFERENCES

[1] A. E. Kalør, R. Guillaume, J. J. Nielsen, A. Mueller, and P. Popovski, "Network slicing in industry 4.0 applications: Abstraction methods and end-to-end analysis," *IEEE Trans. Ind. Informat.*, vol. 14, no. 12, pp. 5419–5427, Dec. 2018.

[2] A. Majumder and J. Caffery, "Power line communications," *IEEE Potentials*, vol. 23, no. 4, pp. 4–8, Oct./Nov. 2004.

[3] C. Cano, A. Pittolo, D. Malone, L. Lampe, A. M. Tonello, and A. G. Dabak, "State of the art in power line communications: From the applications to the medium," *IEEE J. Sel. Areas Commun.*, vol. 34, no. 7, pp. 1935–1952, Jul. 2016.

[4] O. Salman, S. Abdallah, I. H. Elhajj, A. Chehab, and A. Kayssi, "Identity-based authentication scheme for the Internet of Things," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Jun. 2016, pp. 1109–1111.

[5] S. V. Kartalopoulos, "A primer on cryptography in communications," *IEEE Commun. Mag.*, vol. 44, no. 4, pp. 146–151, Apr. 2006.

[6] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, 3rd Quart., 2014.

[7] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[8] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[9] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[10] H.-M. Wang and T.-X. Zheng, *Physical Layer Security in Random Cellular Networks*. Singapore: Springer, 2016.

[11] X. Zhou, R. K. Ganti, and J. G. Andrews, "Secure wireless network connectivity with multi-antenna transmission," *IEEE Trans. Wireless Commun.*, vol. 10, no. 2, pp. 425–430, Feb. 2011.

[12] P. C. Pinto, J. Barros, and M. Z. Win, "Secure communication in stochastic wireless networks—Part I: Connectivity," *IEEE Trans. Inf. Forensics Security*, vol. 7, pp. 125–138, 2012.

[13] P. C. Pinto, J. Barros, and M. Z. Win, "Secure communication in stochastic wireless networks—Part II: Maximum rate and collusion," *IEEE Trans. Inf. Forensics Security*, vol. 7, pp. 139–147, 2012.

[14] W. Wang, K. C. Teh, and K. H. Li, "Artificial noise aided physical layer security in multi-antenna small-cell networks," *IEEE Trans. Inf. Forensics Security*, vol. 12, pp. 1470–1482, 2017.

[15] Y. Ai, A. Mathur, G. D. Verma, L. Kong, and M. Cheffena, "Comprehensive physical layer security analysis of FSO communications over Málaga channels," *IEEE Photon. J.*, vol. 12, no. 6, pp. 1–17, Dec. 2020.

[16] D. Anastasiadou and T. Antonakopoulos, "Multipath characterization of indoor power-line networks," *IEEE Trans. Power Del.*, vol. 20, no. 1, pp. 90–99, Jan. 2005.

[17] M. Zimmermann and K. Dostert, "A multipath model for the powerline channel," *IEEE Trans. Commun.*, vol. 50, no. 4, pp. 553–559, Apr. 2002.

[18] A. Pittolo and A. M. Tonello, "Physical layer security in PLC networks: Achievable secrecy rate and channel effects," in *Proc. 17th IEEE Int. Symp. Power Line Commun. Appl.*, Mar. 2013, pp. 273–278.

[19] A. Pittolo and A. Tonello, "Physical layer security in power line communication networks: An emerging scenario, other than wireless," *IET Commun.*, vol. 8, no. 8, pp. 1239–1247, Jun. 2014.

[20] Y. Zhuang and L. Lampe, "Physical layer security in MIMO power line communication networks," in *Proc. 18th IEEE Int. Symp. Power Line Commun. Appl.*, Mar. 2014, pp. 272–277.

[21] A. Salem, K. A. Hamdi, and E. Alsusa, "Physical layer security over correlated log-normal cooperative power line communication channels," *IEEE Access*, vol. 5, pp. 13909–13921, 2017.

[22] V. Mohan, A. Mathur, V. Aishwarya, and S. Bhargav, "Secrecy analysis of PLC system with channel gain and impulsive noise," in *Proc. IEEE 90th Veh. Technol. Conf. (VTC-Fall)*, Sep. 2019, pp. 1–6.

[23] G. Kaddoum, "Wireless chaos-based communication systems: A comprehensive survey," *IEEE Access*, vol. 4, pp. 2621–2648, 2016.

[24] G. Kaddoum, P. Chargé, D. Roviras, and D. Fournier-Prunaret, "Performance analysis of differential chaos shift keying over an AWGN channel," in *Proc. Int. Conf. Adv. Comput. Tools Eng. Appl.*, Jul. 2009, pp. 255–258.

[25] G. Kaddoum and N. Tadayon, "Differential chaos shift keying: A robust modulation scheme for power-line communications," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 64, no. 1, pp. 31–35, Jan. 2017.

[26] Y. Xia, C. K. Tse, and F. C.-M. Lau, "Performance of differential chaos-shift-keying digital communication systems over a multipath fading channel with delay spread," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 51, no. 12, pp. 680–684, Dec. 2004.

[27] J. Yu and Y.-D. Yao, "Detection performance of chaotic spreading LPI waveforms," *IEEE Trans. Wireless Commun.*, vol. 4, no. 2, pp. 390–396, Mar. 2005.

[28] V. Lynnyk and S. Čelikovskỳ, "On the anti–synchronization detection for the generalized lorenz system and its applications to secure encryption," *Kybernetika*, vol. 46, no. 1, pp. 1–18, 2010.

[29] F. C. Lau, K. Y. Cheong, and C. K. Tse, "Permutation-based DCSK and multiple-access DCSK systems," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, vol. 50, no. 6, pp. 733–742, Jun. 2003.

[30] Y.-S. Lau, K. H. Lin, and Z. M. Hussain, "Space-time encoded secure chaos communications with transmit beamforming," in *Proc. TENCON IEEE Region 10 Conf.*, Nov. 2005, pp. 1–5.

[31] G. Kaddoum, F.-D. Richardson, and F. Gagnon, "Design and analysis of a multi-carrier differential chaos shift keying communication system," *IEEE Trans. Commun.*, vol. 61, no. 8, pp. 3281–3291, Aug. 2013.

[32] G. Kaddoum, F. Gagnon, and F.-D. Richardson, "Design of a secure multi-carrier DCSK system," in *Proc. IEEE Int. Symp. Wireless Commun. Syst. (ISWCS)*, Aug. 2012, pp. 964–968.

[33] L. Kong, G. Kaddoum, and M. Taha, "Performance analysis of physical layer security of chaos-based modulation schemes," in *Proc. IEEE 11th Int. Conf. Wireless Mobile Comput. Netw. Commun. (WiMob)*, Oct. 2015, pp. 283–288.

[34] W. M. Tam, F. C.-M. Lau, and C. K. Tse, "Generalized correlation-delay-shift-keying scheme for noncoherent chaos-based communication systems," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 53, no. 3, pp. 712–721, Mar. 2006.

[35] M. Zheng, T. Huang, L. Wang, and P. Chen, "Performance analysis of M-ary DCSK system over narrow band power-line communications," in *Proc. IEEE 23rd Asia–Pacific Conf. Commun. (APCC)*, Dec. 2017, pp. 1–6.

[36] M. Miao, L. Wang, G. Chen, and W. Xu, "Design and analysis of replica piecewise M-Ary DCSK scheme for power line communications with asynchronous impulsive noise," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 67, no. 12, pp. 5443–5453, Dec. 2020.

[37] R. B. Nelsen, *An Introduction to Copulas*. New York, NY, USA: Springer, 2007.

[38] P. Kumar, "Copula functions and applications in engineering," in *Logistics, Supply Chain and Financial Predictive Analytics*. Singapore: Springer, 2019, pp. 195–209.

[39] S.-H. Huang, M.-N. L. Huang, K. T. Wong, and T.-C. Tseng, "Copula—To model multi-channel fading by correlated but arbitrary Weibull marginals, giving a closed-form outage probability of selection-combining reception," *IET Microw. Antennas Propag.*, vol. 9, no. 15, pp. 1698–1705, Jul. 2015.

[40] S. Sriboonchitta and V. Kreinovich, "Why are FGM copulas successful? A simple explanation," *Adv. Fuzzy Syst.*, vol. 2018, pp. 1–5, May 2018.

[41] M. H. Gholizadeh, H. Amindavar, and J. A. Ritcey, "On the capacity of MIMO correlated Nakagami-*m* fading channels using copula," *EURASIP J. Wireless Commun. Netw.*, vol. 2015, no. 1, pp. 1–11, Dec. 2015.

[42] A. Mathur, M. R. Bhatnagar, and B. K. Panigrahi, "Maximum likelihood decoding of QPSK signal in power line communications over Nakagami-m additive noise," in *Proc. IEEE Int. Symp. Power Line Commun. Appl. (ISPLC)*, Mar. 2015, pp. 7–12.

[43] F. R. Ghadi and G. A. Hodtani, "Copula function-based analysis of outage probability and coverage region for wireless multiple access communications with correlated fading channels," *IET Commun.*, vol. 14, no. 11, pp. 1804–1810, Jul. 2020.

[44] F. R. Ghadi and G. A. Hodtani, "Copula-based analysis of physical layer security performances over correlated Rayleigh fading channels," *IEEE Trans. Inf. Foresics Security*, vol. 16, pp. 431–440, 2021.

[45] G. Kaddoum, F. Gagnon, P. Chargé, and D. Roviras, "A generalized BER prediction method for differential chaos shift keying system through different communication channels," *Wireless Pers. Commun.*, vol. 64, no. 2, pp. 425–437, May 2012.

[46] A. Dubey, R. K. Mallik, and R. Schober, "Performance analysis of a power line communication system employing selection combining in correlated log-normal channels and impulsive noise," *IET Commun.*, vol. 9, no. 1, pp. 1–9, May 2014.

[47] A. Mathur, M. R. Bhatnagar, and B. K. Panigrahi, "PLC performance evaluation with channel gain and additive noise over nonuniform background noise phase," *Wiley Trans. Emerg. Telecommun. Technol.*, vol. 28, no. 5, p. e3131, May 2017.

[48] I. Kostić, "Analytical approach to performance analysis for channel subject to shadowing and fading," *IEE Proc. Commun.*, vol. 152, no. 6, pp. 821–827, Dec. 2005.

[49] H. C. Ferreira, L. Lampe, J. Newbury, and T. G. Swart, *Power Line Communications: Theory and Applications for Narrowband and Broadband Communications Over Power Lines*. Chichester, U.K.: Wiley, Jul. 2011.

[50] Y. H. Ma, P. L. So, and E. Gunawan, "Performance analysis of OFDM systems for broadband power line communications under impulsive noise and multipath effects," *IEEE Trans. Power Del.*, vol. 20, no. 2, pp. 674–682, Apr. 2005.

[51] M. Gotz, M. Rapp, and K. Dostert, "Power line channel characteristics and their effect on communication system design," *IEEE Commun. Mag.*, vol. 42, no. 4, pp. 78–86, Apr. 2004.

[52] A. Mathur, M. R. Bhatnagar, Y. Ai, and M. Cheffena, "Performance analysis of a dual-hop wireless-power line mixed cooperative system," *IEEE Access*, vol. 6, pp. 34380–34392, 2018.

[53] M. Sklar, "Fonctions de repartition an dimensions et leurs marges," *Publ. Inst. Stat. Univ. Paris*, vol. 8, pp. 229–231, Jan. 1959.

[54] G. Pan, C. Tang, X. Zhang, T. Li, Y. Weng, and Y. Chen, "Physical-layer security over non-small-scale fading channels," *IEEE Trans. Veh. Technol.*, vol. 65, no. 3, pp. 1326–1339, Mar. 2016.

[55] S. P. Herath, N. H. Tran, and T. Le-Ngoc, "On optimal input distribution and capacity limit of Bernoulli-Gaussian impulsive noise channels," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2012, pp. 3429–3433.

[56] M. Sheikh-Hosseini, G. A. Hodtani, and M. Molavi-Kakhki, "Capacity analysis of power line communication point-to-point and relay channels," *Trans. Emerg. Telecommun. Technol.*, vol. 27, no. 2, pp. 200–215, Jul. 2016.

[57] H. V. Vu, N. H. Tran, T. V. Nguyen, and S. Hariharan, "Estimating Shannon and constrained capacities of Bernoulli-Gaussian impulsive noise channels in Rayleigh fading," *IEEE Trans. commun.*, vol. 62, no. 6, pp. 1845–1856, Jun. 2014.

[58] K. Wiklundh, P. Stenumgaard, and H. Tullberg, "Channel capacity of Middleton's class a interference channel," *Electron. Lett.*, vol. 45, no. 24, pp. 1227–1229, Nov. 2009.

[59] A. Dubey and R. K. Mallik, "Effect of channel correlation on multihop data transmission over power lines with decode-and-forward relays," *IET Commun.*, vol. 10, no. 13, pp. 1623–1630, Sep. 2016.

[60] A. Salem, K. M. Rabie, K. A. Hamdi, E. Alsusa, and A. M. Tonello, "Physical layer security of cooperative relaying power-line communication systems," in *Proc. Int. Symp. Power Line Commun. Appl. (ISPLC)*, Mar. 2016, pp. 185–189.

[61] X. Zhou, M. R. McKay, B. Maham, and A. Hjørungnes, "Rethinking the secrecy outage formulation: A secure transmission design perspective," *IEEE Commun. Lett.*, vol. 15, no. 3, pp. 302–304, Mar. 2011.

[62] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*. Waltham, MA, USA: Academic, 2014.

VINAY MOHAN received the B.Tech. degree in electronics and communication engineering from Uttarakhand Technical University, Dehradun, India, in 2014, and the M.Tech. degree in digital communication from ABV Indian Institute of Information Technology and Management, Gwalior, India, in 2017. He is currently pursuing the Ph.D. degree with the Department of Electrical Engineering, Indian Institute of Technology, Jodhpur, India. His current research interests include power line communication, digital communication, and physical-layer security.

AASHISH MATHUR (Member, IEEE) received the B.E. degree (Hons.) in electronics and instrumentation engineering from the Birla Institute of Technology and Science Pilani, Pilani, India, in 2011, the M.Tech. degree in telecommunication technology and management from the Indian Institute of Technology (IIT) Delhi, New Delhi, India, in 2013, and the Ph.D. degree in power line communications from the Department of Electrical Engineering, IIT Delhi. Before joining the IIT Delhi, he was a Software Engineer with Intel Technology India Pvt., Ltd., Bengaluru, India. He is currently working as an Assistant Professor with the Department of Electrical Engineering, IIT Jodhpur, India. His research interests include power line communications, visible light communications, and free-space optical communications. He was the recipient of Early Career Research Award in 2019 by Science and Engineering Research Board, Department of Science and Technology, Government of India and was selected as an Exemplary Reviewer of IEEE TRANSACTIONS ON COMMUNICATIONS in 2021.

GEORGES KADDOUM (Member, IEEE) received the bachelor's degree in electrical engineering from the École nationale supérieure de techniques avancées Bretagne, Brest, France, the joint M.S. degree in telecommunications and signal processing (circuits, systems, and signal processing) from the Université de Bretagne Occidentale and Telecom Bretagne, Brest, in 2005, and the Ph.D. degree (Hons.) in signal processing and telecommunications from the National Institute of Applied Sciences, University of Toulouse, Toulouse, France, in 2009. He is currently a Professor and the Tier 2 Canada Research Chair with the École de Technologie Supérieure (ÉTS), Université du Québec, Montreal, Canada. Since 2010, he has been a Scientific Consultant in space and wireless telecommunications for several USA and Canadian companies. He has published more than 300 journals, conference papers, two chapters in books, and eight pending patents. His recent research interests include wireless communication networks, tactical communications, resource allocations, and security. He was a recipient of the best papers awards from the 2014 IEEE International Conference on Wireless and Mobile Computing, Networking, Communications with three coauthors and the 2017 IEEE International Symposium on Personal Indoor and Mobile Radio Communications with four coauthors. He was also a recipient of the IEEE TRANSACTIONS ON COMMUNICATIONS Exemplary Reviewer Award, in 2015, 2017, and 2019; the Research Excellence Award from the Université du Québec in 2018; the Research Excellence Award from ÉTS in recognition of his outstanding research outcomes in 2019. In 2014, he was the ÉTS Research Chair in physical-layer security for wireless networks. He is currently serving as an Area Editor for the IEEE TRANSACTIONS ON MACHINE LEARNING IN COMMUNICATIONS AND NETWORKING and an Associate Editor for the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, IEEE TRANSACTIONS ON COMMUNICATIONS, and IEEE COMMUNICATIONS LETTERS.